**JP2002-232962A**

**MOBILE COMMUNICATION AUTHENTICATION INTERWORKING SYSTEM**

Date of publication of application : 16.08.2002

Application number : 2001-030543

Applicant : KDDI CORP
Date of filing : 07.02.2001

Inventor : OHASHI MASAYOSHI
TANAKA TOSHIAKI
NEMOTO TAKASHI

Abstract:
PROBLEM TO BE SOLVED: To provide a mobile communication authentication interworking system that can efficiently execute CR(Challenge Response) authentication with high security in roaming between systems where a random number transmission bit length differs between networks without revising an existing protocol.
SOLUTION: The interworking system utilizes a configuration that for example, in the case of roaming from an ANSI(American National Standards Institute)-41 system to a GSM(Global System for Mobile Communications), the CR set generated by the home ANSI-41 system is basically included as it is by the GSM system (excess bits are filled by zero or the like) and transmitted to attain communication of a random number and an arithmetic result with a terminal roaming to the GSM system.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－232962
（P2002－232962A）
(43)公開日　平成14年８月16日(2002.8.16)

| (51)Int.Cl.[7] | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｈ０４Ｑ　7/38 | | Ｈ０４Ｂ　7/26 | １０９Ｒ | ５Ｊ１０４ |
| Ｈ０４Ｌ　9/32 | | | １０９Ｇ | ５Ｋ０６７ |
| Ｈ０４Ｑ　7/34 | | Ｈ０４Ｌ　9/00 | ６７５Ｃ | |
| | | Ｈ０４Ｑ　7/04 | Ｃ | |

審査請求　未請求　請求項の数１　ＯＬ　（全　７　頁）

(21)出願番号　特願2001－30543(P2001－30543)

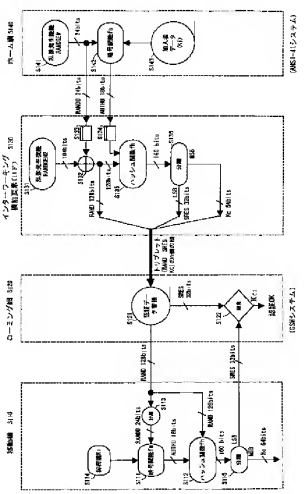
(22)出願日　平成13年２月７日(2001.2.7)

(71)出願人　000208891
ケイディーディーアイ株式会社
東京都新宿区西新宿二丁目３番２号
(72)発明者　大橋　正良
埼玉県上福岡市大原２－１－15　株式会社ケイディディ研究所内
(72)発明者　田中　俊昭
埼玉県上福岡市大原２－１－15　株式会社ケイディディ研究所内
(74)代理人　100069257
弁理士　大塚　学

最終頁に続く

(54)【発明の名称】　移動通信認証インターワーキング方式

(57)【要約】
【課題】既存のプロトコルに変更をきたすことなく、乱数伝達ビット長が網間で異なるシステム間のローミングにおけるＣＲ認証の効率的でかつセキュリティ上安全な実行を可能とする移動通信認証インターワーキング方式を提供する。
【解決手段】例えば、ＡＮＳＩ－４１からＧＳＭへのローミングの場合に、ホームのＡＮＳＩ－４１システムが生成したＣＲ組は、基本的にはそのままＧＳＭシステムに包みこんで（余分なビット分は０等により埋めて）伝送することで乱数，演算結果をＧＳＭシステムにローミングしている端末とやりとりすることが可能であることを利用する構成を有している。



【特許請求の範囲】
【請求項１】　あらかじめ同一の秘密鍵が移動機と該移動機の本来属する移動通信網であるホーム網のデータベース内に設定，記憶されるとともに，該秘密鍵と同一の暗号関数が前記移動機と前記ホーム網に備わっており、該移動機が前記秘密鍵を有していることを、網側から該移動機に乱数を用いて送出し、該移動機ではその乱数と該移動機の前記秘密鍵を前記暗号関数の入力として演算を行った結果を前記移動通信網に返すことで証明することにより、該移動機の正当性を確認するチャレンジ・レスポンス認証方式が実装された移動通信網が存在する系において、
該移動機の移動先の移動通信網であるローミング先網における乱数伝達ビット長が、前記ホーム網で用いられる乱数伝達ビット長よりも長い場合に、両網間をまたがってインターワークを行うインターワーキング機能要素において、乱数発生機能と、安全な一方向性の特徴を有するハッシュ関数を配備し、
前記ホーム網より前記インターワーキング機能要素に送出されたチャレンジ・レスポンスの１組に対して、該インターワーキング機能要素において、適切な個数の乱数ｎ個を発生させ、この乱数とチャレンジを結合させた結果を新たなチャレンジにすると共に、新たなチャレンジならびにレスポンスを前記ハッシュ関数に通すことにより新たなレスポンスを生成し、この過程をｎ回繰り返すことにより、ｎ組のチャレンジ・レスポンスを発生させて、前記ローミング先網に転送して、該ローミング先網においてｎ回の認証を可能にすることを特徴とする移動通信認証インターワーキング方式。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、方式が異なって存在する携帯電話等の複数の移動通信網において、方式の異なる移動網に移動機がアクセス（ローミング）して通信を行おうとする場合、その移動機が当該移動機の本来属するホームの移動網の正当な移動機であることをローミング先の移動網が確認するための、移動通信網の通信制御方式に関する。
【０００２】
【従来の技術】移動通信網を介する通信では、固定系の通信形態とは異なり、無線通信周波を介して相手移動機と接続されるため、接続される移動機が確かに所望の移動機であるかどうかが網側からは必ずしも明確に判明しない。そのため何らかの手法を用いて、網は接続移動機の正当性を確認する必要がある。この正当性確認は認証と呼ばれている。認証に当たっては、無線通信周波が傍受されやすい性質を持っているため、仮に盗聴を受けたとしても、移動機は、後に盗聴者が不正な移動機を用い、正当な移動機の振りをして移動網にアクセスされない工夫が必要になる。
【０００３】このため現在のディジタル移動通信網では、秘密鍵暗号方式に基づくチャレンジ・レスポンス認証（以下ＣＲ認証と呼ぶ）が幅広く用いられている。以下図２を用いて同方式を説明する。ＣＲ認証方式では、移動通信網と移動機は共通の秘密鍵暗号関数ｆを所持する。その秘密鍵暗号関数ｆは２つの変数を持ち、一つは秘密鍵Ｋｉ、一つは乱数ＲＡＮＤである。秘密鍵Ｋｉはパラメータとなるので、この関数出力をｆＫｉ（ＲＡＮＤ）と記し、その結果の値をＳＲＥＳと呼ぶ。
【０００４】移動網は、自網に所属するすべての正当な移動機の秘密鍵（Ｋｉ）を有する（Ｓ１）。秘密鍵（Ｋｉ）としては、移動機すべてに異なった値が割り当てられる。正当な移動機は、それぞれ自らの秘密鍵Ｋｉを、外部からの読み出しの攻撃に対し、たとえばＩＣカードに格納するなど、物理的に安全に保持している（Ｓ２）。
【０００５】ＣＲ認証に際して、移動機はまず自らの移動機番号を移動網に伝える（Ｓ３）。移動網はデータベース検索によって、対象移動機の秘密鍵Ｋｉを得る。移動網は、乱数（チャレンジ）ＲＡＮＤを発生し（Ｓ４）、移動機に送出する（Ｓ５）。移動機は受け取った乱数ＲＡＮＤと自分の秘密鍵より関数ｆを用いて暗号演算を行い（Ｓ６）、その演算結果（レスポンス）をＳＲＥＳとして移動網に送り返す（Ｓ７）。移動網もＫｉ，ｆを有するので、同じ演算を行う（Ｓ８）。その結果が移動機より送り返されてきたＳＲＥＳと一致すれば（ＹＥＳ）、認証成功であり、さもなくば失敗（ＮＯ）となる。
【０００６】ＣＲ認証では、移動機が正当な秘密鍵Ｋｉを有していることを、無線区間上で直接移動網に提示することなく、ＲＡＮＤとＳＲＥＳの受け渡しのみで移動網に示すことができるため、盗聴によってもＫｉを知られることのない有効な方式である。さらにＲＡＮＤは移動網によって任意に調べ、その値に応じて移動機が返す正しいＳＲＥＳの値は異なるため、複数回不正な移動機が傍受を行っても、自らが正当な移動機になりすますことはできない。従って、ＣＲ認証は、移動通信システムのセキュリティを確保する観点から非常に優れた方式の一つである。以下の説明では、すべてＣＲ認証を用いると仮定する。
【０００７】次にローミングについて説明を行う。ローミングとは、移動機が自網以外の網にアクセスして通信を行う機能をいう。このとき移動機が本来属している網をホーム網、現在アクセスしている網をローミング先網と呼ぶ。ローミング時には、ローミング先網は通信に先立ち、アクセスしてきた移動機がホーム網に正当に登録された移動機であるかどうかを認証する必要がある。しかしながら、ローミング先網は、ローミングしてきた移動機の秘密鍵を持たず、また必ずしもホーム網と同一の暗号関数ｆを採用しているわけではない。ただし、両網

で共通のＣＲ認証スキームを採用し、チャレンジ，レスポンスいずれも同じ情報長を有している場合には、ホーム網が対象となる移動機の秘密鍵Ｋｉ を用いて認証に必要な一つもしくは複数のチャレンジ・レスポンスの組（以下ＣＲ組と呼ぶ）〔ＲＡＮＤ，ＳＲＥＳ〕を生成し、ローミング先網に渡せば、網からチャレンジＲＡＮＤを移動機に投げかけ、移動機より返された結果がホーム網より受け取ったＳＲＥＳと合致するか否かを検証することで、ホーム網と同様に認証を行うことができる。これは現在のＧＳＭ（Global System for Mobile Communications ）システムにおいて広く用いられている方式である。

【０００８】

【発明が解決しようとする課題】上記のようにローミング時にＣＲ組を渡す方式は、各網の暗号関数ｆの一致を必要としない優れた方式である。しかしながら、例えば北米標準であるＡＮＳＩ－４１のようなシステムにおいては、一度にホーム網よりローミング先ネットワークに渡せるＣＲ組が１組（これはユニークチャレンジと呼ばれる）であるのに対し、例えば欧州標準であるＧＳＭシステムでは、複数組を一度に渡すことが可能になっている。ＧＳＭシステムにて複数のチャレンジ・レスポンスを渡すためにインターワーキング機能要素を介し、ＡＮＳＩ－４１システムにて複数のメッセージを送受するのはプロトコルの面からは非常に非効率である。

【０００９】本発明は、既存のプロトコルに変更をきたすことなく、このような乱数伝達ビット長が網間で異なるシステム間のローミングにおけるＣＲ認証の効率的でかつセキュリティ上安全な実行を可能とする移動通信認証インターワーキング方式を提供することを目的としている。

【００１０】

【課題を解決するための手段】本発明によれば上述の問題点は前記特許請求の範囲に記載した手段により解決される。すなわち、本発明は、あらかじめ同一の秘密鍵が移動機と該移動機の本来属する移動通信網であるホーム網のデータベース内に設定，記憶されるとともに、該秘密鍵と同一の暗号関数が前記移動機と前記ホーム網に備わっており、該移動機が前記秘密鍵を有していることを、網側から該移動機に乱数を用いて送出し、該移動機ではその乱数と該移動機の前記秘密鍵を前記暗号関数の入力として演算を行った結果を前記移動通信網に返すことで証明することにより、該移動機の正当性を確認するチャレンジ・レスポンス認証方式が実装された移動通信網が存在する系において、該移動機の移動先の移動通信網であるローミング先網における乱数伝達ビット長が、前記ホーム網で用いられる乱数伝達ビット長よりも長い場合に、両網間をまたがってインターワークを行うインターワーキング機能要素において、乱数発生機能と、安全な一方向性の特徴を有するハッシュ関数を配備し、前記ホーム網より前記インターワーキング機能要素に送出されたチャレンジ・レスポンスの１組に対して、該インターワーキング機能要素において、適切な個数の乱数ｎ個を発生させ、この乱数とチャレンジを結合させた結果を新たなチャレンジにすると共に、新たなチャレンジならびにレスポンスを前記ハッシュ関数に通すことにより新たなレスポンスを生成し、この過程をｎ回繰り返すことにより、ｎ組のチャレンジ・レスポンスを発生させて、前記ローミング先網に転送して、該ローミング先網においてｎ回の認証を可能にすることを特徴とする構成を有している。

【００１１】〔発明の原理〕ＡＮＳＩ－４１システムにて使用される乱数，演算結果はそれぞれ、２４ビット，１８ビットである。またＧＳＭシステムにて使用される乱数，演算結果は１２８ビット，３２ビットである。本発明は、例えば、ＡＮＳＩ－４１からＧＳＭへのローミングの場合に着目すると、ホームのＡＮＳＩ－４１システムが生成したＣＲ組は、基本的にはそのままＧＳＭシステムに包みこんで（余分なビット分は０等により埋めて）伝送することで乱数，演算結果をＧＳＭシステムにローミングしている端末とやりとりすることが可能であることを利用するものである。

【００１２】

【発明の実施の形態】以下本発明の作用等に関し、実施例に基づいてさらに詳細に説明する。

【００１３】〔実施例１〕図１は、ＡＮＳＩ－４１からＧＳＭシステムにローミングを行う際の実施例を示している。本例では、ホーム網Ｓ１４０および移動機Ｓ１１０は暗号関数ｆａ（Ｓ１４２ならびにＳ１１１）を有するものとし、その共通の秘密鍵をＫｉ とする。Ｋｉ はホーム網においては、安全な加入者データベースＳ１４３に、移動機においては安全なメモリＳ１１４に格納されているものとする。ホーム網における乱数ＲＡＮＤＵのビット長は２４ビット、演算結果ＡＵＴＨＵのビット長は１８ビットとする。

【００１４】一方、ローミング先網（Ｓ１２０）のＧＳＭでの乱数ＲＡＮＤのビット長は１２８ビット、演算結果ＳＲＥＳビット長は３２ビットとする。インターワーキングを司る機能要素ＩＩＦ（Interworking and Interoperability Function）Ｓ１３０および移動機Ｓ１１０は、セキュリティ上安全な一方向性の性質を有するハッシュ関数ｆｈ（Ｓ１３５およびＳ１１２）を有するものとし、任意の長さのビット列より、ある長さの安全なハッシュ結果を生成できるものとする。ここではハッシュ関数を例えばＳＨＡ－１とし、その出力を１６０ビットとする。加えて移動機Ｓ１１０とインターワーキング機能要素（ＩＩＦ）Ｓ１３０において暗号化のための鍵Ｋｃは６４ビット長とする。

【００１５】移動機がローミング先ＧＳＭ網Ｓ１２０においてローミング要求を発すると、ローミング先ＧＳＭ

網Ｓ１２０は移動機番号を得てホーム網Ｓ１４０に通知する。ＡＮＳＩ－４１ホーム網Ｓ１４０はそのデータベースＳ１４３中より対応する移動機の秘密鍵Ｋｉを取り出す。実際のＡＮＳＩ－４１システムでは、Ｋｉに相当するものは真の鍵に各種識別子を付加した値になるが、ここではこれらを含めてＫｉと記す。次いでＡＮＳＩ－４１ホーム網Ｓ１４０は、ユニークチャレンジと呼ばれる一組の乱数ＲＡＮＤＵならびに演算結果

【数１】

$$AUTHU = fa\ Ki\ (RANDU) \quad \cdots\cdots(1)$$

$$RANDi = RANDi \parallel RANDU \quad \cdots\cdots(2)$$

$$SRESi = LSB32bits\ of\ \{fh(RANDU, AUTHU)\} = LSB32bits\ of\ \{fh(RANDi \parallel RANDU, fa\ Ki(RANDU))\} \quad \cdots\cdots(3)$$

$$Kci = MSB64bit\ of\ \{fh(RANDi, AUTHU)\} = MSB64bit\ of\ \{fh(RANDi \parallel RANDU, fa\ Ki(RANDU))\}\ (i=1,\cdots n) \quad \cdots(4)$$

（‖は結合を表し、図１ではＳ１３２に対応するトリプレット［ＲＡＮＤｉ，ＳＲＥＳｉ，Ｋｃｉ］（ｉ＝１…，ｎ）のｎ個の組）

をインターワーキング機能要素（ＩＩＦ）Ｓ１３０にて生成する。（ＩＩＦ）Ｓ１３０はこれらをローミング先ＧＳＭ網Ｓ１２０に送付する。

【００１７】ローミング網Ｓ１２０ではこれらのトリプレットをデータベースＳ１２１に格納しておき、認証が必要になる度にこれらのトリプレットを１組ずつ取り出し、ＲＡＮＤｉを移動機Ｓ１１０に対して送出する。移動機Ｓ１１０は、受信した１２８ビットのＲＡＮＤｉを（ＩＩＦ）Ｓ１３０での結合規則Ｓ１３２に則り、Ｓ１１３にて２４ビットのＲＡＮＤＵを抽出する。

【００１８】移動機Ｓ１１０にはＫｉがＳ１１４に格納されているため、式（１）に従いＡＵＴＨＵを計算した後、式（３），（４）に従い、ＳＲＥＳｉ，Ｋｃｉを作成し、ＳＲＥＳｉをローミング網Ｓ１２０に返す。ローミング網Ｓ１２０には（ＩＩＦ）Ｓ１２０より送付されてきたＳＲＥＳｉがあるので、Ｓ１２２にて移動機Ｓ１１０から送付された値と照合を行い、値が一致すれば認証成功であり、一致しなければ失敗となる。認証成功の際には、Ｋｃｉがこの後暗号通信を行うためのセッション鍵を与える。トリプレットは使い捨てである。認証がｎ回行われると、ローミング網Ｓ１２０中のトリプレットを使い尽くすため、新規にインターワーキング機能要素（ＩＩＦ）Ｓ１３０にトリプレット送付要求を送る。

（ＩＩＦ）Ｓ１３０は再びＡＮＳＩ－４１ホーム網Ｓ１４０に対して初期登録と同じ要求を行い、ユニークチャレンジ情報を得てｎ組のトリプレットを作成し、以下同様の処理を継続する。

【００１９】なお、本発明例では移動機を１なる機能要素して取り扱ったが、例えばＧＳＭシステムでは、認証演算は移動機に装着されるＳＩＭ（Subscriber Identity Module）と呼ばれるＩＣカード中に格納されている。この場合も、ＳＩＭが本発明における移動機の機能を果を発生し、インターワーキング機能要素（ＩＩＦ）Ｓ１３０に転送する。

【００１６】インターワーキング機能要素（ＩＩＦ）Ｓ１３０では、これらの値をレジスタＳ１３３，Ｓ１３４に保持しておく。次にＳ１３０に配置された乱数発生器Ｓ１３１により、ＧＳＭ網が要求する組数ｎだけの１０４ビットの乱数（ＲＮＤ１，ＲＮＤ２，…ＲＮＤｎ）を発生させ、

【数２】

たすことにより、本発明が実施可能である。

【００２０】インターワーキング機能要素（ＩＩＦ）Ｓ１３０ならびに移動機Ｓ１１０にはハッシュ関数ｆｈが用いられているが、もしこの関数ｆｈを公知にしておきたくない場合には、あらかじめシステムに決められた秘密鍵Ｋｈを用意しておき、（ＩＩＦ）Ｓ１３０ならびに移動機Ｓ１１０内にこの値を格納し、式（３），（４）の処理にて、ｆｈ（ＲＡＮＤｉ，ＡＵＴＨＵ）を、ｆｈ（ＲＡＮＤｉ，ＡＵＴＨＵ，Ｋｈ）とすればよい。

【００２１】

【発明の効果】以上述べたように、本発明による移動通信認証方式を用いることにより、インターワーキング機能要素において一個のＡＮＳＩ－４１用のＣＲ組から、安全に複数のＧＳＭシステム用ＣＲ組を生成することができるため、ＡＮＳＩ－４１／ＧＳＭのいずれのシステムにも変更を来すことなく、ＡＮＳＩ－４１からＧＳＭへの認証インターワーキングが可能となる。

【００２２】また安全性の面からは、新たに生成されたｎ個のトリプレットから、ホーム網の加入者に関する秘密情報を探り出すことは極めて困難である。すなわち、ｎ個のトリプレットに含まれるＳＲＥＳｉ，Ｋｃｉは、安全な一方向性ハッシュ関数の出力であるため、仮に無線区間に盗聴者がいるものとして、観測されるＲＡＮＤｉ，ＳＲＥＳｉより入力値ＡＵＴＨＵを探り出すのは大変困難である。たとえこれが割り出されたとしても、そこで利用するのは（ＲＡＮＤＵ，ＡＵＴＨＵ）という、通常のＡＮＳＩ－４１におけるユニークチャレンジ相当の情報である。従ってこの状況においてさえ、通常のＡＮＳＩ－４１と同等のセキュリティが確保されているといえる。

【００２３】なお例１においては対象をＡＮＳＩ－４１システムからＧＳＭシステムへのローミングとして説明を加えたが、基本的にチャレンジ・レスポンスをベースとするシステム間の認証インターワークで、かつローミング先システムの乱数伝達長がホーム網における乱数伝

達長に比べて長い場合には、本発明が適用可能である。

【図面の簡単な説明】

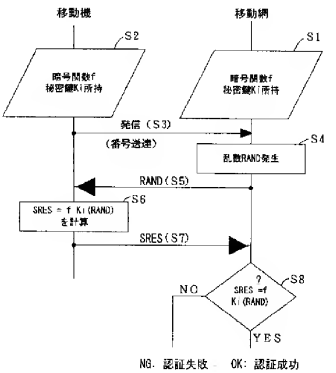
【図１】本発明の構成及び動作を説明するための動作フローを含むブロック図である。

【図２】本発明に用いるチャレンジ・レスポンス認証方式を説明するためのフロー図である。

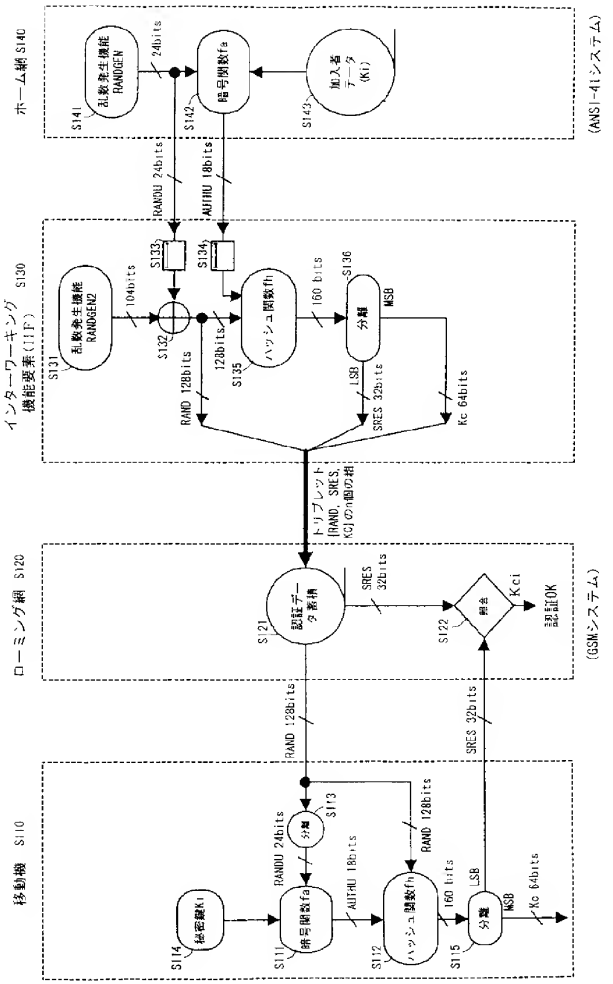
【符号の説明】

Ｓ１１０　移動機
Ｓ１１１　暗号関数ｆａ
Ｓ１１２　ハッシュ関数ｆｈ
Ｓ１１３　分離回路
Ｓ１１４　秘密鍵Ｋｉ
Ｓ１１５　分離回路
Ｓ１２０　ローミング網（ＧＳＭシステム）
Ｓ１２１　認証データ蓄積
Ｓ１２２　照合回路
Ｓ１３０　インターワーキング機能要素（ＩＩＦ）
Ｓ１３１　乱数発生機能（ＲＡＮＤＧＥＮＺ）
Ｓ１３２　結合規則
Ｓ１３３，Ｓ１３４　レジスタ
Ｓ１３５　ハッシュ関数ｆｈ
Ｓ１３６　分離器
Ｓ１４０　ホーム網（ＡＮＳＩ－４１）
Ｓ１４１　乱数発生機能（ＲＡＮＤＧＥＮ）
Ｓ１４２　暗号関数ｆａ
Ｓ１４３　加入者データ（Ｋｉ）

【図２】



【図１】


移動機 S10
ローミング網 S120
インターワーキング機能要素(IIF) S130
ホーム網 S140
(GSMシステム)
(ANSI-41システム)
S114 秘密鍵Ki
S111 認証関数fa
S112 ハッシュ関数fh
S113 分離
S115 分離
RAND 128bits
RAND 24bits
AUTHU 18bits
160 bits
LSB
MSB
Kc 64bits
SRES 32bits
S121 認証データ要求
S122 照合
Kci
認証OK
トリプレット(RAND, SRES, Kc)のHLR引渡
S131 乱数発生機能 RANDGEN2
104bits
S132
S133
S134
S135
S136 分離
S140
S141 乱数発生機能 RANDGEN
24bits
S142 暗号関数fa
S143 加入者データ(Ki)

フロントページの続き

(72)発明者　根本　隆史
埼玉県上福岡市大原２－１－15　株式会社
ケイディディ研究所内

Ｆターム(参考)　5J104 AA04 AA07 KA02 KA04 KA06
KA08 KA21 NA03 NA11 NA12
NA22 PA02
5K067 AA33 BB04 DD17 EE04 EE10
HH11 HH17 HH21 HH23